IT SECURITY POLICY

Applicable to the students and staff

Author: Head of Digital Transformation
Approved by: SLT
Date: Aug 2025
Review date: Aug 2027

Contents

1 INTRODUCTION

1.1 The College Group use a large amount of information in order to operate effectively and the majority of this information is in electronic format and held on computers and in our IT systems. It is essential that this information is managed effectively so that it remains secure, accessible to authorised users and its integrity is protected. The IT Security Policy sets standards outlining the way electronic information and IT systems should be managed and operated to ensure the College Group complies with its obligations in relation to IT Security. The policy sets out how all users of College Group IT systems and the information they contain must act to ensure these standards and obligations are met.

2 POLICY STATEMENT

2.1 The College Group recognises the importance of keeping its information and IT systems secure and protected from unauthorised use. Through compliance with this policy, the College Group will ensure that all corporate information generated, used and held electronically in IT systems, networks, media and related forms is accurate, secure and available to authorised users for business purposes when needed.

3 SCOPE

3.1 The IT Security Policy covers all internal College Group systems and connections to wider networks. It sets out how information contained within or accessible via those IT systems should be handled to ensure it remains secure. It should be read in conjunction with our other IT related policies. All internally and approved externally hosted systems must conform to this policy. The College Group reserves the right to isolate any IT system including externally hosted service or networks, which represents a potential or actual breach of security; to monitor information sent over its networks; and to deny user access to the College Group and its subsidiaries, approved IT systems.

4. RESPONSIBILITIES

4.1 This policy applies to all students, employees, including temporary, casual, contract and agency staff, as well as any contractors, guest and visitors acting on behalf of the College Group.

5. RELATIONSHIP TO OTHER POLICIES

5.1 This policy must be read in conjunction with the following policies:

- IT Acceptable Use Policy
- Use of College Email Policy
- Data Protection Policy and Procedure
- CCTV Policy
- Mobile Phone Policy and Procedure (applicable only to staff)

6. PERMITTED USE

6.1 All users of IT facilities must adhere to the rules set out in this IT Security Policy. Users are also required to conform to the current IT Acceptable Use Policy (which they are obliged to agree to on first using the network) and the JANET Acceptable Use Policy. (JANET, formerly Joint Academic Network, is the high-speed network for the UK

research and education community and provides our access to the Internet.)

7. USER AUTHORISATION

7.1 The College Group will ensure that all computer users are formally authorised to use the network and an audit trail of authorisation is maintained. Students are authorised through the enrolment process and staff through the HR process. Use of network Guest accounts are only permitted under 'exceptional' circumstances. Guests (or staff who are expecting guests) who need to use our facilities (especially out of normal working hours) should liaise with IT, well in advance of arrival, to book suitable equipment and assistance.

8. USER ACCOUNTS AND PASSWORDS

8.1 Individual users will each be given a personal College Group account for which they are held responsible. The account is for the sole use of the authorised user for access to the College Group's IT facilities. Users must not permit their account to be used by anyone else and users must not use or attempt to use someone else's account. Passwords must not be shared, written down or stored on or near a computer. If a user forgets their password, they must go to the Self-Service Password Reset web page or to one of the four college's IT Helpdesks. Users can change their own passwords without administrator intervention, either on College Group computers by using the Change Password application from the Start menu, by pressing Alt-Ctrl-Delete and selecting Change a password or through the self-service password service. Users must follow good security practices when selecting passwords. Passwords should be at least twelve characters in length and should be made from three random words.

8.2 If users suspect that a password may be known to an unauthorised party, the password should be changed immediately and not used ever again. It is good practice to use a different password for your College Group account than any personal/private accounts.

9. ID CARDS/ACCESS CONTROL CARDS

9.1 Lost or misplaced identity cards present a security risk because the information they contain may allow an unauthorised user in possession of the card to gain access to somewhere/something they shouldn't. The loss of cards used for controlling access to buildings can lead to a breach of physical security. To guard against such events, if cards are lost or stolen, users must report the loss to the IT Helpdesk at the earliest opportunity. The reported lost card will immediately be disabled. Users must follow relevant procedures for a replacement card to be issued. If a lost card is found, the card must be handed in to the IT Helpdesk. The relevant user will be informed that the card has been found. If the loss has not already been reported, the user should also attend the IT Helpdesk for a new card to be issued. The lost card will not be returned to a user; a new one will always be issued. The old card must be physically destroyed to ensure information contained in it is not accessible after it has been disposed of.

10. KEEPING INFORMATION SECURE

10.1 Individuals who use the College Group's computer systems to process personal data must comply with the requirements of the Data Protection Act and GDPR as set out in the Data Protection Policy. For mobile devices such as tablet computers, ipads, smartphones etc; the user must ensure the device PIN or password has been set and

that the device is set to automatically lock after a short period of inactivity. This will help protect the device against misuse and is an extra safeguard for any personal contact details or any other confidential information held on the device should it fall into the wrong hands; however this does not replace the need for encryption. Any device without a PIN or password as a minimum-security measure must not be used to hold any organisational information. Users should note that if a device is lost or damaged, the information stored on it may not be recoverable. These types of devices should therefore never be used to store the only copy of information. Where encryption is used, decryption passwords must be kept securely and separately. Encrypted information cannot be accessed without the encryption password. Any personal data sent to other organisations should be sent in an encrypted, password protected "Zip" file.

10.2 The College Group takes IT security very seriously and complies with the Data Protection Act 1998 and UK General Data Protection Regulation (UK GDPR), the principles of which state that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner
b) Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed
d) Accurate, and where necessary kept up to date
e) Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
g) Kept for no longer than necessary for the particular purpose
h) Processed in accordance with the rights of individuals.

11. PHISHING AND SPAM

11.1 Information security involves technical security measures but also requires users to ensure they act appropriately to maintain the security of computer systems and the corporate network.

11.2 Attacks will be made on these systems and networks by unauthorised parties with the aim of obtaining organisational information or causing damage or disruption to that information or those systems by infecting them with viruses. Users should be aware of such attacks and be able to recognise them in order to stop them being successful. Attacks may involve phone calls from individuals trying to obtain confidential information by deception or may occur by email. Users must ensure that organisational information is only disclosed by phone to callers who are authorised and entitled to receive that information.

11.3 Users must ensure that they do not click on links in spam or phishing emails or emails which appear to be such; attachments to such emails must not be opened. Users must never email their usernames and passwords in response to emails purporting to be from IT Services; IT Services staff will never ask for users' passwords.

11.4 Spam and phishing emails are becoming more and more sophisticated and plausible, if in any doubt, do not open the mail and delete it or the IT Helpdesk for advice.

12. BACK UP AND RECOVERY

12.1 Students and Staff are advised to use their allocated OneDrive for Business area for storing of files (or SharePoint Online/Teams for shared staff files) as these areas are backed up daily by IT Services systems.

12.2 All organisational information must be stored on the network or in Office 365, to ensure it is available for use, backed up and recoverable in the event of an incident.

12.3 Users must not store organisational information on individual computers or devices unless exceptional circumstances apply, following advice from IT Services and the Data Protection Officer (where personal data is involved).

12.4 IT Services system administrators cannot and do not back up files held away from the College's network.

13. CLOUD SERVICES

13.1 Users must follow the College Group's Data Protection Policy when handling data. The cloud storage services approved for use are Blackboard, Onefile and Microsoft Office 365, including Microsoft OneDrive. A full security and compliance risk assessment has been undertaken for Microsoft's Online Services. Users of these services need to be aware that IT Services has no direct control over the availability of cloud services, as they are hosted by 3rd parties. Responsibility for the availability, backup and recovery of these services lies with those 3rd parties. Deleted files from Microsoft Office 365 can be retrieved by the account holder for up to 90 days after which the data may be recoverable by the administrator, however after 180 days it is lost. Microsoft carry out periodic updates and maintenance, which may result in loss of service for a period.

14. SOCIAL NETWORKING

14.1 Students should not use their College Group email addresses on their private social media accounts as this may compromise the security and privacy of the College Group's email system and the information it contains. The exception to this requirement is where accounts are used for interaction in genuine academic circles.

15. REMOTE WORKING

15.1 Users must note that when using home PCs or other equipment at fixed locations outside the College, they are operating outside the College's IT security perimeter.

15.2 In these situations, users must not assume their own PC equipment is protected by the same security measures as standard PC equipment routinely used at the college and directly managed by IT Services. Users must be aware that weak security on home PCs used for home working could lead to College Group account passwords becoming known to unauthorised parties, which could lead to security incidents involving college IT systems.

15.3 It is vital that PCs used for home working are themselves properly secured and it is the responsibility of users to ensure that is so (see list below).

15.4 Users are responsible for safeguarding the equipment against unauthorised access, misuse, theft, or loss when in their home or in transit, for example on public transport

or in their vehicle.

15.5 Users are also responsible for ensuring that where the equipment is used by others (e.g. family members), no organisational information is accessible by such unauthorised parties.

15.6 Users must ensure that all reasonable protection measures are in place and operating where applicable, as follows: (IT Services IT Helpdesk team are able to provide assistance and advice)

- The computer's local Firewall should be enabled
- Anti-virus software is set to automatically update itself
- Anti-spyware software to provide continuous protection against malicious software being downloaded
- Up to date security patches must be installed for both the operating system and applications when they are released by software vendors. Doing so will help protect the equipment against security vulnerabilities that have been identified.
- Wireless networks at home must be properly secured against eavesdropping and intrusion.

15.7 Users must comply with the security requirements of this document at all times and where personal data is being processed, they must also comply with the Data Protection Policy. Users must not access internal or confidential/sensitive information over unsecured broadband or public wireless networks, including cyber cafes, as these present a security risk.

15.8 Users should also be aware of the physical environment when working remotely ensuring no one is looking over their shoulder at information on screen.

16. COPYRIGHT

16.1 Copyrighted and licensed software must not be duplicated, removed or added by users unless it is explicitly stated that this is acceptable. The College Group's IT systems and network infrastructure, including wireless must not be used for the downloading or streaming of copyrighted materials including, but not limited to video and audio files, without the written consent of the owner or copyright-holder.

17. USE OF SOFTWARE

17.1 Copyrighted and licensed software may not be copied or distributed by users in contravention of the licensing agreement. Users are not permitted to trial software, for example from a removable disk on College Group computers, and are not permitted to modify the operating system either manually or by downloading applications such as screensavers, themes etc.

17.2 Personal use of peer-to-peer networking and file sharing applications is not permitted on any of the College's systems.

These applications use College Group resources for non-college purposes, they increase the risk of virus infection and spyware which compromise privacy and security and they involve legal risks regarding the storage of copyrighted material.

18 NETWORK MONITOR AND AUDITING

18.1 Computer logs are records of past events on a computer system. Logs can and are used to aid investigations into security incidents and misuse of the College Group's IT systems. Types of information recorded in computer logs include (but are not limited to):

- The dates and times of account logins and logouts
- Internet use and email traffic
- The behaviour and health of the computer system itself

18.2 Use of computer accounts and Internet usage will be logged and recorded in order to comply with our JANET contract. Software logs will be enabled as appropriate to comply with license conditions. Where appropriate, computer systems will always log user activity to provide an audit trail so that actions can be traced back to individual's, for example, when there is a case of suspected misuse. Attempts to breach security will be investigated immediately. IT Services system administrators periodically review computer logs to detect attempts to breach system security. Where checks of computer logs raise suspicions of attacks on the computer system, actual security breaches or other irregularities, IT Services will promptly investigate such concerns.

19 SECURITY BEACHES

19.1 All users must report actual or suspected security breaches to the Director of Digital Transformation and IT, or Head of Digital Transformation and the College Group's Data Protection Officer as soon as they become aware of it, whether they have caused the breach or they are informed of the breach by another party.

19.2 IT Services will ensure that any security breaches reported to them are acted upon promptly and will keep appropriate records and documentation, in line with UK GDPR guidelines. Corrective actions taken, measures to avoid a reoccurrence and other resolutions will be documented and monitored.

19.3 In cases where an incident involves personal data, it must be reported to the Data Protection Officer (dpo@ucscollegegroup.ac.uk) without delay, as it is likely that the ICO will need to be informed and that must take place within 72 non-working hours of the College becoming aware of the breach.

Here are some common examples of a data breach:

- Access by an unauthorised third party
- Deliberate or accidental action by a data processor
- Sending personal data to an incorrect recipient by email
- Mobile devices (such as laptop, ipad, or phone) containing personal data, being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

20 REVIEW OF POLICY

20.1 This policy will be reviewed every two years or earlier if required.